Cryptanalysis of Multivariate and Odd-Characteristic HFE Variants

Luk Bettale[1] Jean-Charles Faugère Ludovic Perret

LIP6 - SALSA
UPMC, CNRS, INRIA Paris-Rocquencourt

to be presented at PKC 2011

Séminaire SALSA, December 2010

[1] author partially supported by DGA/MRIS

Outline

Introduction

- Presentation of HFE/Multi-HFE
- Known attacks
- The MinRank Problem

Attack on Multi-HFE

- Improvement and Extension of Kipnis-Shamir's attack
- Complexity Analysis
- Attacks on Multi-HFE Variants
- Experimental results

Conclusion

- Summary

Outline

Introduction

- Presentation of HFE/Multi-HFE
- Known attacks
- The MinRank Problem

Attack on Multi-HFE

- Improvement and Extension of Kipnis-Shamir's attack
- Complexity Analysis
- Attacks on Multi-HFE Variants
- Experimental results

Conclusion

- Summary

History of Hidden Field Equations (HFE)

- Patarin 1996
- Multivariate Cryptography
- Generalization of C^*
- Encryption/Signature.

Tsutomu Matsumoto and Hideki Imai.
Public quadratic polynomial-tuples for efficient signature-verification and message-encryption.
In *Advances in Cryptology – EUROCRYPT '88*.

Jacques Patarin.
Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of asymmetric algorithms.
In *Advances in Cryptology – EUROCRYPT '96*.

Multi-HFE

- Generalization of HFE
- Using a multivariate system in the big field
- Using odd-characteristic to prevent algebraic attack
- Various additional variants.


Olivier Billet, Jacques Patarin, and Yannick Seurin.
Analysis of Intermediate Field Systems.
In *SCC 2008*.


Chia-Hsin Owen Chen, Ming-Shing Chen, Jintai Ding, Fabian Werner, and Bo-Yin Yang.
Odd-char multivariate Hidden Field Equations.
Cryptology ePrint Archive, 2008.


Anna Inn-Tung Chen, Ming-Shing Chen, Tien-Ren Chen, Chen-Mou Cheng, Jintai Ding, Eric Li-Hsiang Kuo, Frost Yu-Shuang Lee, and Bo-Yin Yang.
SSE implementation of multivariate PKCs on modern x86 CPUs.
In *Cryptographic Hardware and Embedded Systems – CHES 2009*.

Hidden Field Equations

$\varphi : \mathbb{F}_{q^n} \to (\mathbb{F}_q)^n.$

Secret key

$F : (\mathbb{F}_{q^n}) \to (\mathbb{F}_{q^n})$

$$F(X) = \sum_{\substack{0 \leqslant i \leqslant j \leqslant n-1 \\ q^i + q^j \leqslant D}} A_{i,j} X^{q^i + q^j} + \sum_{\substack{0 \leqslant i \leqslant n-1 \\ q^i \leqslant D}} B_i X^{q^i} + C$$

$S, T \in \mathrm{Aff}(n, \mathbb{F}_q).$

Public system of equations

$G : (\mathbb{F}_q)^n \to (\mathbb{F}_q)^n$

$$G(x_1, \ldots, x_n) = (T \circ \varphi \circ F \circ \varphi^{-1} \circ S)(x_1, \ldots, x_n).$$

Hidden Field Equations

$\varphi : \mathbb{F}_{q^n} \to (\mathbb{F}_q)^n$.

Secret key

$F : (\mathbb{F}_{q^n}) \to (\mathbb{F}_{q^n})$

$$F(X) = \sum_{\substack{0 \leqslant i \leqslant j \leqslant n-1 \\ q^i + q^j \leqslant D}} A_{i,j} X^{q^i + q^j} + \sum_{\substack{0 \leqslant i \leqslant n-1 \\ q^i \leqslant D}} B_i X^{q^i} + C$$

$S, T \in \mathrm{Aff}(n, \mathbb{F}_q)$.

Public system of equations

$G : (\mathbb{F}_q)^n \to (\mathbb{F}_q)^n$

$$G(x_1, \ldots, x_n) = (T \circ \varphi \circ F \circ \varphi^{-1} \circ S)(x_1, \ldots, x_n).$$

Encrypt: $\underline{c} = G(\underline{m})$. message $\underline{m} \in (\mathbb{F}_q)^n$

Hidden Field Equations

$\varphi : \mathbb{F}_{q^n} \to (\mathbb{F}_q)^n$.

Secret key

$F : (\mathbb{F}_{q^n}) \to (\mathbb{F}_{q^n})$

$$F(X) = \sum_{\substack{0 \leqslant i \leqslant j \leqslant n-1 \\ q^i + q^j \leqslant D}} A_{i,j} X^{q^i + q^j} + \sum_{\substack{0 \leqslant i \leqslant n-1 \\ q^i \leqslant D}} B_i X^{q^i} + C$$

$S, T \in \mathrm{Aff}(n, \mathbb{F}_q)$.

Decrypt: $\underline{m} = S^{-1} \circ \varphi \circ F^{-1} \circ \varphi^{-1} \circ T^{-1}(\underline{c})$.

Public system of equations

$G : (\mathbb{F}_q)^n \to (\mathbb{F}_q)^n$

$$G(x_1, \ldots, x_n) = (T \circ \varphi \circ F \circ \varphi^{-1} \circ S)(x_1, \ldots, x_n).$$

Encrypt: $\underline{c} = G(\underline{m})$. message $\underline{m} \in (\mathbb{F}_q)^n$

Hidden Field Equations

$\varphi : (\mathbb{F}_{q^d})^N \to (\mathbb{F}_q)^n$, with $n = Nd$.

Secret key

$F : (\mathbb{F}_{q^d})^N \to (\mathbb{F}_{q^d})^N$

$$F_k(X_1, \ldots, X_N) = \sum_{1 \leqslant i \leqslant j \leqslant N} \sum_{\substack{0 \leqslant u,v \leqslant d-1 \\ q^u + q^v \leqslant D}} A_{k,i,u,j,v} X_i^{q^u} X_j^{q^v} + \sum_{1 \leqslant i \leqslant N} \sum_{\substack{0 \leqslant u \leqslant d-1 \\ q^u \leqslant D}} B_{k,i,u} X_i^{q^u} + C_k.$$

$S, T \in \mathrm{Aff}(n, \mathbb{F}_q)$.

Decrypt: $\underline{m} = S^{-1} \circ \varphi \circ F^{-1} \circ \varphi^{-1} \circ T^{-1}(\underline{c})$.

Public system of equations

$G : (\mathbb{F}_q)^n \to (\mathbb{F}_q)^n$

$$G(x_1, \ldots, x_n) = (T \circ \varphi \circ F \circ \varphi^{-1} \circ S)(x_1, \ldots, x_n).$$

Encrypt: $\underline{c} = G(\underline{m})$. message $\underline{m} \in (\mathbb{F}_q)^n$

Hidden Field Equations

$\varphi : (\mathbb{F}_{q^d})^N \to (\mathbb{F}_q)^n$, with $n = Nd$.

Secret key

$F : (\mathbb{F}_{q^d})^N \to (\mathbb{F}_{q^d})^N$

$$F_k(X_1, \ldots, X_N) = \sum_{1 \leqslant i \leqslant j \leqslant N} A_{k,i,j} X_i X_j + \sum_{1 \leqslant i \leqslant N} B_{k,i} X_i + C_k.$$

$S, T \in \mathrm{Aff}(n, \mathbb{F}_q)$.

Decrypt: $\underline{m} = S^{-1} \circ \varphi \circ F^{-1} \circ \varphi^{-1} \circ T^{-1}(\underline{c})$.

Public system of equations

$G : (\mathbb{F}_q)^n \to (\mathbb{F}_q)^n$

$$G(x_1, \ldots, x_n) = (T \circ \varphi \circ F \circ \varphi^{-1} \circ S)(x_1, \ldots, x_n).$$

Encrypt: $\underline{c} = G(\underline{m})$. message $\underline{m} \in (\mathbb{F}_q)^n$

Parameters for Multi-HFE

Table: Proposed parameters for HFE/Multi-HFE.

	q	N	d	D	expected security
HFE	2	1	128	513	128
PHFE	7	1	67	56	201
IFS	2	8	16	2	128
THFE	31	3	10	2	150

Outline

Introduction
- Presentation of HFE/Multi-HFE
- Known attacks
- The MinRank Problem

Attack on Multi-HFE
- Improvement and Extension of Kipnis-Shamir's attack
- Complexity Analysis
- Attacks on Multi-HFE Variants
- Experimental results

Conclusion
- Summary

Algebraic attack

HFE: $q = 2$, $N = 1$.

Message recovery

Given a ciphertext $\underline{c} = (c_1, \ldots, c_n)$, solve the quadratic system

$$\begin{aligned} g_1(x_1, \ldots, x_n) - c_1 &= 0, \\ &\vdots \\ g_n(x_1, \ldots, x_n) - c_n &= 0. \end{aligned}$$


Jean-Charles Faugère and Antoine Joux.
Algebraic cryptanalysis of Hidden Field Equation (HFE) cryptosystems using Gröbner bases.
In *Advances in Cryptology – CRYPTO 2003*.


Louis Granboulan, Antoine Joux, and Jacques Stern.
Inverting HFE is quasipolynomial.
In *Advances in Cryptology – CRYPTO 2006*.

Algebraic attack

HFE: $q = 2$, $N = 1$.

Message recovery

Given a ciphertext $\underline{c} = (c_1, \ldots, c_n)$, solve the quadratic system

$$\begin{aligned} g_1(x_1, \ldots, x_n) - c_1 &= 0, \\ &\vdots \\ g_n(x_1, \ldots, x_n) - c_n &= 0. \end{aligned}$$

- Use field equations
- Degree of reg. $\approx \log_q(D)$.

Jean-Charles Faugère and Antoine Joux.
Algebraic cryptanalysis of Hidden Field Equation (HFE) cryptosystems using Gröbner bases.
In *Advances in Cryptology – CRYPTO 2003*.

Louis Granboulan, Antoine Joux, and Jacques Stern.
Inverting HFE is quasipolynomial.
In *Advances in Cryptology – CRYPTO 2006*.

Key recovery attack on HFE: $N = 1$.

Univariate representation ($G \in \mathbb{F}_{q^n}[X]$)

$$G = T \circ \varphi \circ F \circ \varphi^{-1} \circ S \qquad \rightsquigarrow \qquad G(X) = T(F(S(X))).$$

Use interpolation.

Aviad Kipnis and Adi Shamir.
Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization.
In *Advances in Cryptology – CRYPTO '99*.

Key recovery attack on HFE: $N = 1$.

Univariate representation ($G \in \mathbb{F}_{q^n}[X]$)

$$G = T \circ \varphi \circ F \circ \varphi^{-1} \circ S \qquad \rightsquigarrow \qquad G(X) = T(F(S(X))).$$

Use interpolation.

Matrix representation (non-standard quadratic forms)

$$G(X) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} g_{i,j} X^{q^i+q^j} = \underline{X} \mathbf{G} \underline{X}^t$$

with $\underline{X} = (X, X^q, \ldots, X^{q^{n-1}})$.

We have that $\mathrm{rank}(\mathbf{G}) = \log_q(\deg(G))$.

Aviad Kipnis and Adi Shamir.
Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization.
In *Advances in Cryptology – CRYPTO '99*.

Matrix representation (non-standard quadratic forms)

$$F(X) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} f_{i,j} X^{q^i+q^j} = \underline{X}\mathbf{F}\underline{X}^t$$

with $\underline{X} = (X, X^q, \ldots, X^{q^{n-1}})$.

We have that $\mathrm{rank}(\mathbf{F}) = \log_q(\deg(F))$.

Matrix representation (non-standard quadratic forms)

$$F(X) = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} f_{i,j} X^{q^i+q^j} = \underline{X}\mathbf{F}\underline{X}^t$$

with $\underline{X} = (X, X^q, \ldots, X^{q^{n-1}})$.

We have that $\mathrm{rank}(\mathbf{F}) = \log_q(\deg(F))$.

$$\begin{pmatrix} f_{1,1} & \cdots & f_{1,\ell} & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ldots & \vdots \\ f_{\ell,1} & \cdots & f_{\ell,\ell} & 0 & \ldots & 0 \\ 0 & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ldots & \vdots \\ 0 & \ldots & 0 & 0 & \ldots & 0 \end{pmatrix}$$

Fundamental equation

$$\sum_{k=0}^{n-1} t_k \mathbf{G}^{*k} = \mathbf{W}\mathbf{F}\mathbf{W}^t$$

with $G^{q^k} = \underline{X}\,\mathbf{G}^{*k}\,\underline{X}$ and $\mathbf{W} = [s^{q^i}_{j-i}]$.

Fundamental equation

$$\sum_{k=0}^{n-1} t_k \mathbf{G}^{*k} = \mathbf{W}\mathbf{F}\mathbf{W}^t$$

with $G^{q^k} = \underline{X}\,\mathbf{G}^{*k}\,\underline{X}$ and $\mathbf{W} = [s_{j-i}^{q^i}]$.

Find $t_k \in \mathbb{F}_{q^n}$ such that

$$\operatorname{rank}\left(\sum_{k=0}^{n-1} t_k \mathbf{G}^{*k}\right) = \log_q(D).$$

Fundamental equation

$$\sum_{k=0}^{n-1} t_k \mathbf{G}^{*k} = \mathbf{W}\mathbf{F}\mathbf{W}^t$$

with $G^{q^k} = \underline{X}\,\mathbf{G}^{*k}\,\underline{X}$ and $\mathbf{W} = [s_{j-i}^{q^i}]$.

Find $t_k \in \mathbb{F}_{q^n}$ such that

$$\operatorname{rank}\left(\sum_{k=0}^{n-1} t_k \mathbf{G}^{*k}\right) = \log_q(D).$$

- Allows to recover the transformation T
- The MinRank problem on matrices over $\mathbb{F}_{q^n}$.

Kipnis-Shamir attack: recover S

Recovering the transformation S

$$\ker\left(\sum_{k=0}^{n-1} t_k \mathbf{G}^{*k}\right) = \ker(\mathbf{W}\mathbf{F}\mathbf{W})$$

$$\ker\left(\sum_{k=0}^{n-1} t_k \mathbf{G}^{*k}\right) = \ker(\mathbf{W}\mathbf{F})$$

$$\ker\left(\sum_{k=0}^{n-1} t_k \mathbf{G}^{*k}\right)\mathbf{W} = \ker(\mathbf{F})$$

- $\ker(\mathbf{F})$ has zeroes on first columns
- Recover $\mathbf{W}$ = solve a linear system
- Still feasible in characteristic 2 ?

Xin Jiang, Jintai Ding, and Lei Hu.
Kipnis-Shamir attack on HFE revisited.
In *Information Security and Cryptology*, 2007.

Summary

Algebraic attack

- Needs field equations
- Not practical in big characteristic fields.

Kipnis-Shamir Attack

- Not for Multi-HFE
- Does not work as presented in characteristic 2
- Theoretical attack.

Summary

Algebraic attack

- Needs field equations
- Not practical in big characteristic fields.

Kipnis-Shamir Attack

- Not for Multi-HFE
- Does not work as presented in characteristic 2
- Theoretical attack.

Key recovery attack on Multi-HFE ?

Outline

Introduction
- Presentation of HFE/Multi-HFE
- Known attacks
- The MinRank Problem

Attack on Multi-HFE
- Improvement and Extension of Kipnis-Shamir's attack
- Complexity Analysis
- Attacks on Multi-HFE Variants
- Experimental results

Conclusion
- Summary

MinRank (MR)

Input: $n, r, k \in \mathbb{N}$ and $\mathbf{M_0}, \mathbf{M_1}, \ldots, \mathbf{M_k} \in \mathscr{M}_{n\times n}(\mathbb{K})$.
Question: is there a k-tuple $(\lambda_1, \ldots, \lambda_k)$ of elements in $\mathbb{K}$ such that: $\mathrm{Rank}\left(\left(\sum_{i=1}^{k} \lambda_i \mathbf{M_i}\right) - \mathbf{M_0}\right) \leqslant r$.

- Computational MinRank is NP-hard
- Reduces to solve a multivariate polynomial system.

W. Buss, G. Frandsen, and J. Shallit
The computational complexity of some problems of linear algebra.
In *Journal of Computer and System Sciences* 1999.

Kernel Modeling (Kipnis-Shamir)

Solve $n(n-r)$ quadratic equations in $r(n-r)+k$ variables.

$$\begin{pmatrix} 1 & & & x_{1,1} & \dots & x_{1,r} \\ & \ddots & & \vdots & & \vdots \\ & & 1 & x_{n-r,1} & \dots & x_{n-r,r} \end{pmatrix} \cdot \left(\left(\sum_{i=1}^{k} \lambda_i \mathbf{M_i} \right) - \mathbf{M_0} \right) = \mathbf{0}.$$

Minors modeling

Solve $\binom{n}{r+1}^2$ equations (high degree) in k variables coming from

$$\text{Minors} \left(\left(\sum_{i=1}^{k} \lambda_i \mathbf{M_i} \right) - \mathbf{M_0}, r+1 \right) = 0$$

Kernel Modeling (Kipnis-Shamir)

Solve $n(n-r)$ quadratic equations in $r(n-r)+k$ variables.

$$\begin{pmatrix} 1 & & & x_{1,1} & \dots & x_{1,r} \\ & \ddots & & \vdots & & \vdots \\ & & 1 & x_{n-r,1} & \dots & x_{n-r,r} \end{pmatrix} \cdot \left(\left(\sum_{i=1}^{k} \lambda_i \mathbf{M_i} \right) - \mathbf{M_0} \right) = \mathbf{0}.$$

Minors modeling

Solve $\binom{n}{r+1}^2$ equations (high degree) in k variables coming from

$$\text{Minors}\left(\left(\sum_{i=1}^{k} \lambda_i \mathbf{M_i} \right) - \mathbf{M_0}, r+1 \right) = 0$$

Used as a black box !

Outline

Introduction
- Presentation of HFE/Multi-HFE
- Known attacks
- The MinRank Problem

Attack on Multi-HFE
- Improvement and Extension of Kipnis-Shamir's attack
- Complexity Analysis
- Attacks on Multi-HFE Variants
- Experimental results

Conclusion
- Summary

HFE: $N = 1$.
Public key: $G = T \circ \varphi \circ F \circ \varphi^{-1} \circ S$.

Change basis matrix

Let $(\theta_1, \ldots, \theta_d)$ be a vector basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

$$\mathbf{M} = \begin{pmatrix} \theta_1 & \theta_1^q & \ldots & \theta_1^{q^{d-1}} \\ \theta_2 & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ \theta_d & \ldots & \ldots & \theta_d^{q^{d-1}} \end{pmatrix}.$$

- $\varphi^{-1} : (x_1, \ldots, x_n) \to \big((x_1, \ldots, x_n)\mathbf{M}\big)[1]$.
- $\varphi : X \to (X, \ldots, X^{q^{n-1}})\mathbf{M}^{-1}$.

Rewriting as matrix operations

Proposition

$$G = T \circ \varphi \circ F \circ \varphi^{-1} \circ S$$

Rewriting as matrix operations

Proposition

$$\begin{aligned} G &= T \circ \varphi \circ F \circ \varphi^{-1} \circ S \\ (\mathbf{G_1}, \ldots, \mathbf{G_n}) &= (\mathbf{S}\mathbf{M}\mathbf{F}^{*0}\mathbf{M}^t\mathbf{S}^t, \ldots, \mathbf{S}\mathbf{M}\mathbf{F}^{*n-1}\mathbf{M}^t\mathbf{S}^t)\mathbf{M}^{-1}\mathbf{T} \end{aligned}$$

Proposition

$$
\begin{aligned}
G &= T \circ \varphi \circ F \circ \varphi^{-1} \circ S \\
(\mathbf{G_1}, \ldots, \mathbf{G_n}) &= (\mathbf{S}\mathbf{M}\mathbf{F}^{*0}\mathbf{M}^t\mathbf{S}^t, \ldots, \mathbf{S}\mathbf{M}\mathbf{F}^{*n-1}\mathbf{M}^t\mathbf{S}^t)\mathbf{M}^{-1}\mathbf{T} \\
(\mathbf{G_1}, \ldots, \mathbf{G_n})\mathbf{T}^{-1}\mathbf{M} &= (\mathbf{S}\mathbf{M}\mathbf{F}^{*0}\mathbf{M}^t\mathbf{S}^t, \ldots, \mathbf{S}\mathbf{M}\mathbf{F}^{*n-1}\mathbf{M}^t\mathbf{S}^t)
\end{aligned}
$$

Proposition

$$
\begin{aligned}
G &= T \circ \varphi \circ F \circ \varphi^{-1} \circ S \\
(\mathbf{G_1}, \ldots, \mathbf{G_n}) &= (\mathbf{S}\mathbf{M}\mathbf{F}^{*0}\mathbf{M}^t\mathbf{S}^t, \ldots, \mathbf{S}\mathbf{M}\mathbf{F}^{*n-1}\mathbf{M}^t\mathbf{S}^t)\mathbf{M}^{-1}\mathbf{T} \\
(\mathbf{G_1}, \ldots, \mathbf{G_n})\mathbf{T}^{-1}\mathbf{M} &= (\mathbf{S}\mathbf{M}\mathbf{F}^{*0}\mathbf{M}^t\mathbf{S}^t, \ldots, \mathbf{S}\mathbf{M}\mathbf{F}^{*n-1}\mathbf{M}^t\mathbf{S}^t) \\
(\mathbf{G_1}, \ldots, \mathbf{G_n})\mathbf{U} &= (\mathbf{W}\mathbf{F}^{*0}\mathbf{W}^t, \ldots, \mathbf{W}\mathbf{F}^{*n-1}\mathbf{W}^t).
\end{aligned}
$$

Proposition

$$
\begin{aligned}
G &= T \circ \varphi \circ F \circ \varphi^{-1} \circ S \\
(\mathbf{G_1}, \ldots, \mathbf{G_n}) &= (\mathbf{S}\mathbf{M}\mathbf{F}^{*0}\mathbf{M}^t\mathbf{S}^t, \ldots, \mathbf{S}\mathbf{M}\mathbf{F}^{*n-1}\mathbf{M}^t\mathbf{S}^t)\mathbf{M}^{-1}\mathbf{T} \\
(\mathbf{G_1}, \ldots, \mathbf{G_n})\mathbf{T}^{-1}\mathbf{M} &= (\mathbf{S}\mathbf{M}\mathbf{F}^{*0}\mathbf{M}^t\mathbf{S}^t, \ldots, \mathbf{S}\mathbf{M}\mathbf{F}^{*n-1}\mathbf{M}^t\mathbf{S}^t) \\
(\mathbf{G_1}, \ldots, \mathbf{G_n})\mathbf{U} &= (\mathbf{W}\mathbf{F}^{*0}\mathbf{W}^t, \ldots, \mathbf{W}\mathbf{F}^{*n-1}\mathbf{W}^t).
\end{aligned}
$$

Theorem (Fundamental equation)

$$\sum_{k=0}^{n-1} u_{k,0}\mathbf{G_{k+1}} = \mathbf{W}\mathbf{F}\mathbf{W}^t$$

with $F^{q^k} = \underline{X}\,\mathbf{F}^{*k}\,\underline{X}$.

Proposition

$$
\begin{aligned}
G &= T \circ \varphi \circ F \circ \varphi^{-1} \circ S \\
(\mathbf{G_1}, \ldots, \mathbf{G_n}) &= (\mathbf{S}\mathbf{M}\mathbf{F}^{*0}\mathbf{M}^t\mathbf{S}^t, \ldots, \mathbf{S}\mathbf{M}\mathbf{F}^{*n-1}\mathbf{M}^t\mathbf{S}^t)\mathbf{M}^{-1}\mathbf{T} \\
(\mathbf{G_1}, \ldots, \mathbf{G_n})\mathbf{T}^{-1}\mathbf{M} &= (\mathbf{S}\mathbf{M}\mathbf{F}^{*0}\mathbf{M}^t\mathbf{S}^t, \ldots, \mathbf{S}\mathbf{M}\mathbf{F}^{*n-1}\mathbf{M}^t\mathbf{S}^t) \\
(\mathbf{G_1}, \ldots, \mathbf{G_n})\mathbf{U} &= (\mathbf{W}\mathbf{F}^{*0}\mathbf{W}^t, \ldots, \mathbf{W}\mathbf{F}^{*n-1}\mathbf{W}^t).
\end{aligned}
$$

Theorem (Fundamental equation)

$$\sum_{k=0}^{n-1} u_{k,0}\mathbf{G_{k+1}} = \mathbf{W}\mathbf{F}\mathbf{W}^t$$

with $F^{q^k} = \underline{X}\,\mathbf{F}^{*k}\,\underline{X}$.

Entries of matrices in $\mathbb{F}_q \rightsquigarrow$ faster solving.

Change basis matrix for Multi-HFE

Let $(\theta_1, \ldots, \theta_d)$ a basis of $\mathbb{F}_{q^d}$ over $\mathbb{F}_q$.

$$\mathbf{M} = \begin{pmatrix} \theta_1 & \theta_1^q & \ldots & \theta_1^{q^{d-1}} & & & & \\ \theta_2 & \ddots & & \vdots & & & & \\ \vdots & & \ddots & \vdots & & & 0 & \\ \theta_d & \ldots & \ldots & \theta_d^{q^{d-1}} & & & & \\ & & & & \ddots & & & \\ & & & & & \theta_1 & \theta_1^q & \ldots & \theta_1^{q^{d-1}} \\ & & 0 & & & \theta_2 & \ddots & & \vdots \\ & & & & & \vdots & & \ddots & \vdots \\ & & & & & \theta_d & \ldots & \ldots & \theta_d^{q^{d-1}} \end{pmatrix}$$

- $\varphi^{-1} : (x_1, \ldots, x_n) \to \big((x_1, \ldots, x_n)\,\mathbf{M}\big)[1, d+1, \ldots, (N-1)\,d+1]$.
- $\varphi : (X_1, \ldots, X_N) \to (X_1, \ldots, X_1^{q^{d-1}}, \ldots, X_N, \ldots, X_N^{q^{d-1}})\,\mathbf{M}^{-1}$.

Extension of the attack

Proposition

$$G = T \circ \varphi \circ F \circ \varphi^{-1} \circ S$$

Proposition

$$G = T \circ \varphi \circ F \circ \varphi^{-1} \circ S$$

$$(\mathbf{G_1}, \ldots, \mathbf{G_n}) = (\mathbf{SMF_1}^{*0}\mathbf{M}^t\mathbf{S}^t, \ldots, \mathbf{SMF_N}^{*d-1}\mathbf{M}^t\mathbf{S}^t)\mathbf{M}^{-1}\mathbf{T}$$

Proposition

$$
\begin{aligned}
G &= T \circ \varphi \circ F \circ \varphi^{-1} \circ S \\
(\mathbf{G_1}, \ldots, \mathbf{G_n}) &= (\mathbf{S}\mathbf{M}\mathbf{F_1}^{*0}\mathbf{M}^t\mathbf{S}^t, \ldots, \mathbf{S}\mathbf{M}\mathbf{F_N}^{*d-1}\mathbf{M}^t\mathbf{S}^t)\mathbf{M}^{-1}\mathbf{T} \\
(\mathbf{G_1}, \ldots, \mathbf{G_n})\mathbf{T}^{-1}\mathbf{M} &= (\mathbf{S}\mathbf{M}\mathbf{F_1}^{*0}\mathbf{M}^t\mathbf{S}^t, \ldots, \mathbf{S}\mathbf{M}\mathbf{F_N}^{*d-1}\mathbf{M}^t\mathbf{S}^t)
\end{aligned}
$$

Proposition

$$
\begin{aligned}
G &= T \circ \varphi \circ F \circ \varphi^{-1} \circ S \\
(\mathbf{G_1}, \ldots, \mathbf{G_n}) &= (\mathbf{S}\mathbf{M}\mathbf{F_1}^{*0}\mathbf{M}^t\mathbf{S}^t, \ldots, \mathbf{S}\mathbf{M}\mathbf{F_N}^{*d-1}\mathbf{M}^t\mathbf{S}^t)\mathbf{M}^{-1}\mathbf{T} \\
(\mathbf{G_1}, \ldots, \mathbf{G_n})\mathbf{T}^{-1}\mathbf{M} &= (\mathbf{S}\mathbf{M}\mathbf{F_1}^{*0}\mathbf{M}^t\mathbf{S}^t, \ldots, \mathbf{S}\mathbf{M}\mathbf{F_N}^{*d-1}\mathbf{M}^t\mathbf{S}^t) \\
(\mathbf{G_1}, \ldots, \mathbf{G_n})\mathbf{U} &= (\mathbf{W}\mathbf{F_1}^{*0}\mathbf{W}^t, \ldots, \mathbf{W}\mathbf{F_N}^{*d-1}\mathbf{W}^t).
\end{aligned}
$$

Proposition

$$
\begin{aligned}
G &= T \circ \varphi \circ F \circ \varphi^{-1} \circ S \\
(\mathbf{G_1}, \ldots, \mathbf{G_n}) &= (\mathbf{S}\mathbf{M}\mathbf{F_1}^{*0}\mathbf{M}^t\mathbf{S}^t, \ldots, \mathbf{S}\mathbf{M}\mathbf{F_N}^{*d-1}\mathbf{M}^t\mathbf{S}^t)\mathbf{M}^{-1}\mathbf{T} \\
(\mathbf{G_1}, \ldots, \mathbf{G_n})\mathbf{T}^{-1}\mathbf{M} &= (\mathbf{S}\mathbf{M}\mathbf{F_1}^{*0}\mathbf{M}^t\mathbf{S}^t, \ldots, \mathbf{S}\mathbf{M}\mathbf{F_N}^{*d-1}\mathbf{M}^t\mathbf{S}^t) \\
(\mathbf{G_1}, \ldots, \mathbf{G_n})\mathbf{U} &= (\mathbf{W}\mathbf{F_1}^{*0}\mathbf{W}^t, \ldots, \mathbf{W}\mathbf{F_N}^{*d-1}\mathbf{W}^t).
\end{aligned}
$$

Theorem (Fundamental equations)

$$
\sum_{k=0}^{n-1} u_{k,0}\mathbf{G_{k+1}} = \mathbf{W}\mathbf{F_1}\mathbf{W}^t, \ldots, \sum_{k=0}^{n-1} u_{k,N}\mathbf{G_{k+1}} = \mathbf{W}\mathbf{F_N}\mathbf{W}^t
$$

with $F^{q^k} = \underline{X}\,\mathbf{F}^{*k}\,\underline{X}$.

Proposition

$$
\begin{aligned}
G &= T \circ \varphi \circ F \circ \varphi^{-1} \circ S \\
(\mathbf{G_1}, \ldots, \mathbf{G_n}) &= (\mathbf{S}\mathbf{M}\mathbf{F_1}^{*0}\mathbf{M}^t\mathbf{S}^t, \ldots, \mathbf{S}\mathbf{M}\mathbf{F_N}^{*d-1}\mathbf{M}^t\mathbf{S}^t)\mathbf{M}^{-1}\mathbf{T} \\
(\mathbf{G_1}, \ldots, \mathbf{G_n})\mathbf{T}^{-1}\mathbf{M} &= (\mathbf{S}\mathbf{M}\mathbf{F_1}^{*0}\mathbf{M}^t\mathbf{S}^t, \ldots, \mathbf{S}\mathbf{M}\mathbf{F_N}^{*d-1}\mathbf{M}^t\mathbf{S}^t) \\
(\mathbf{G_1}, \ldots, \mathbf{G_n})\mathbf{U} &= (\mathbf{W}\mathbf{F_1}^{*0}\mathbf{W}^t, \ldots, \mathbf{W}\mathbf{F_N}^{*d-1}\mathbf{W}^t).
\end{aligned}
$$

Theorem (Fundamental equations)

$$
\sum_{k=0}^{n-1} u_{k,0}\mathbf{G_{k+1}} = \mathbf{W}\mathbf{F_1}\mathbf{W}^t, \ldots, \sum_{k=0}^{n-1} u_{k,N}\mathbf{G_{k+1}} = \mathbf{W}\mathbf{F_N}\mathbf{W}^t
$$

with $F^{q^k} = \underline{X}\,\mathbf{F}^{*k}\,\underline{X}$.

- N MinRank relations
- Only one to be solved !

Outline

Introduction

- Presentation of HFE/Multi-HFE
- Known attacks
- The MinRank Problem

Attack on Multi-HFE

- Improvement and Extension of Kipnis-Shamir's attack
- Complexity Analysis
- Attacks on Multi-HFE Variants
- Experimental results

Conclusion

- Summary

Proposition (Faugère, Safey El Din, Spaenlehauer)

For a MinRank instance with parameters n,r,k:

$$D_{reg} \leqslant 1 + \deg\left(\mathrm{HS}(t)\right)$$

with

$$\mathrm{HS}(t) = \left[(1-t)^{(n-r)^2-k} \, \frac{\det \mathbf{A}(t)}{t^{\binom{r}{2}}} \right]$$

and $\mathbf{A} = [a_{i,j}]$ a $(r \times r)$-matrix with $a_{i,j}(t) = \sum_{\ell=0}^{n-\max(i,j)} \binom{n-i}{\ell}\binom{n-j}{\ell} t^{\ell}$.

Jean-Charles Faugère, Mohab Safey El Din, and Pierre-Jean Spaenlehauer
Computing loci of rank defects of linear matrices using Gröbner bases and applications to cryptology.
In *Proceedings of the International Symposium on Symbolic and Algebraic Computation – ISSAC 2010*.

Complexity of the attack

Conjecture (verified for a wide range of parameters)

For a MinRank coming from Multi-HFE with parameters q, N, d, D

$$D_{reg} \leqslant N \log(D) + 1.$$

Proposition

Assuming the conjecture, the complexity of solving the Multi-HFE MinRank is

$$\mathcal{O}\left(d^{(N \log_q(D)+1)\,\omega}\right)$$

with $2 \leqslant \omega < 3$ *the linear algebra constant.*

The complexity is polynomial in d, the degree of the extension.

Complexity

$$\mathcal{O}\left(d^{(N\log_q(D)+1)\,\omega}\right).$$

Similar keys

Two HFE parameter sets (q_1, N_1, d_1, D_1) and (q_2, N_2, d_2, D_2) are similar iff

- $q_1 = q_2$ (same ground field)
- $N_1\, d_1 = N_2\, d_2$ (same public key size)
- $N_1 \log_{q_1}(D_1) = N_2 \log_{q_2}(D_2)$ (same private key size).

Two similar parameter sets have the same key bit-size.

Weakness of Multi-HFE

Complexity

$$\mathcal{O}\left(d^{(N\log_q(D)+1)\,\omega}\right).$$

Similar keys

Two HFE parameter sets (q_1, N_1, d_1, D_1) and (q_2, N_2, d_2, D_2) are similar iff

- $q_1 = q_2$ (same ground field)
- $N_1\, d_1 = N_2\, d_2$ (same public key size)
- $N_1 \log_{q_1}(D_1) = N_2 \log_{q_2}(D_2)$ (same private key size).

Two similar parameter sets have the same key bit-size.

- Bigger $N \rightsquigarrow$ more efficient attack.

Complexity

$$\mathcal{O}\left(d^{(N\log_q(D)+1)\,\omega}\right).$$

Similar keys

Two HFE parameter sets (q_1, N_1, d_1, D_1) and (q_2, N_2, d_2, D_2) are similar iff

- $q_1 = q_2$ (same ground field)
- $N_1\, d_1 = N_2\, d_2$ (same public key size)
- $N_1 \log_{q_1}(D_1) = N_2 \log_{q_2}(D_2)$ (same private key size).

Two similar parameter sets have the same key bit-size.

- Bigger $N \rightsquigarrow$ more efficient attack.
- The MinRank problem has N degrees of freedom.

Outline

Introduction
- Presentation of HFE/Multi-HFE
- Known attacks
- The MinRank Problem

Attack on Multi-HFE
- Improvement and Extension of Kipnis-Shamir's attack
- Complexity Analysis
- Attacks on Multi-HFE Variants
- Experimental results

Conclusion
- Summary

Equivalent keys

Equivalent keys for HFE and Multi-HFE.

Proposition

Let (F, S, T) *a Multi-HFE private key, if* $A, B \in \mathrm{Aff}(N, \mathbb{F}_{q^d})$ *are invertible, then*

- $((B \circ F \circ A), A^{-1} \circ S, T \circ B^{-1})$ *is an equivalent key*
- $(F(X^{q^{d-k}})^{q^k}, \mathrm{Frob_k} \circ S, T \circ \mathrm{Frob_{d\text{-}k}})$ *is an equivalent key.*

where $\mathrm{Frob_k} : (\mathbb{F}_{q^d})^N \to (\mathbb{F}_{q^d})^N$ *sends* $(X_1, \ldots, X_N)$ *to* $(X_1^{q^k}, \ldots, X_N^{q^k})$.

Equivalent keys

Equivalent keys for HFE and Multi-HFE.

Proposition

Let (F, S, T) a Multi-HFE private key, if $A, B \in \mathrm{Aff}(N, \mathbb{F}_{q^d})$ are invertible, then

- $((B \circ F \circ A), A^{-1} \circ S, T \circ B^{-1})$ *is an equivalent key*
- $(F(X^{q^{d-k}})^{q^k}, \mathrm{Frob_k} \circ S, T \circ \mathrm{Frob_{d\text{-}k}})$ *is an equivalent key.*

where $\mathrm{Frob_k} : (\mathbb{F}_{q^d})^N \to (\mathbb{F}_{q^d})^N$ *sends* $(X_1, \ldots, X_N)$ *to* $(X_1^{q^k}, \ldots, X_N^{q^k})$.

Theorem

The MinRank problem from Multi-HFE can be solved by fixing N coefficients at random.

Equivalent keys

Equivalent keys for HFE and Multi-HFE.

Proposition

Let (F, S, T) a Multi-HFE private key, if $A, B \in \mathrm{Aff}(N, \mathbb{F}_{q^d})$ are invertible, then

- $((B \circ F \circ A), A^{-1} \circ S, T \circ B^{-1})$ *is an equivalent key*
- $(F(X^{q^{d-k}})^{q^k}, \mathrm{Frob_k} \circ S, T \circ \mathrm{Frob_{d\text{-}k}})$ *is an equivalent key.*

where $\mathrm{Frob_k} : (\mathbb{F}_{q^d})^N \to (\mathbb{F}_{q^d})^N$ *sends* $(X_1, \ldots, X_N)$ *to* $(X_1^{q^k}, \ldots, X_N^{q^k})$.

Theorem

The MinRank problem from Multi-HFE can be solved by fixing N coefficients at random.

- Only $(n - N + 1)$ public polynomials are needed
- Attack the minus variant.

Multi-HFE$^-$ (signature)

Private key: Unchanged.
Public key: $\mathbf{s}$ equations removed $\rightsquigarrow$ under-determined system.

- When $\mathbf{s} < N$, MinRank with no additional cost !
- Adapt the recovery of the matrix $\mathbf{T}$.

$$\mathbf{K} \cdot \left(\sum_{i=1}^{n} \lambda_i \mathbf{G_i} \right) = \mathbf{0}.$$

Multi-HFE$^-$ (signature)

Private key: Unchanged.
Public key: $\mathbf{s}$ equations removed $\rightsquigarrow$ under-determined system.

- When $\mathbf{s} < N$, MinRank with no additional cost !
- Adapt the recovery of the matrix $\mathbf{T}$.

$$\mathbf{K} \cdot \left(\sum_{i=1}^{n-N+1} \lambda_i \mathbf{G_i} + \sum_{i=1}^{N-1} \lambda_{n-N+1+i} \mathfrak{G}_\mathbf{i} \right) = \mathbf{0}.$$

Multi-HFE$^-$ (signature)

Private key: Unchanged.
Public key: $\mathbf{s}$ equations removed $\rightsquigarrow$ under-determined system.

- When $\mathbf{s} < N$, MinRank with no additional cost !
- Adapt the recovery of the matrix $\mathbf{T}$.

$$\mathbf{K} \cdot \left(\sum_{i=1}^{n-N} \lambda_i \mathbf{G_i} + \sum_{i=1}^{N-1} \ell_i \mathfrak{G}_\mathbf{i} \right) = \mathbf{0}.$$

Attack on Multi-HFE with embedding

Multi-HFE with embedding (encryption)

Private key: additional embedding $\rho : \mathbb{F}_q^{n-r} \to (\mathbb{F}_q)^n$.
Public key: $\mathbf{r}$ variables less $\rightsquigarrow$ over-determined system.

Attack on Multi-HFE with embedding

Multi-HFE with embedding (encryption)

Private key: additional embedding $\rho : \mathbb{F}_q^{n-r} \to (\mathbb{F}_q)^n$.
Public key: $\mathbf{r}$ variables less $\rightsquigarrow$ over-determined system.

Ideas of the attack:

- Solve MinRank on $(n - \mathbf{r} \times n - \mathbf{r})$-matrices
- Recover a matrix $\mathbf{S}$ without the big field structure.
- More details in the paper.

Outline

Introduction
- Presentation of HFE/Multi-HFE
- Known attacks
- The MinRank Problem

Attack on Multi-HFE
- Improvement and Extension of Kipnis-Shamir's attack
- Complexity Analysis
- Attacks on Multi-HFE Variants
- Experimental results

Conclusion
- Summary

Table: Attack on Multi-HFE variants with parameters $q = 31$, $N = 3$, $d = 8$, $D = 2$ (≈ 120 bits security).

	MR time	d_{reg}	recover $\mathbf{U}$	recover $\mathbf{W}$
No variant (ref. time)	23.3 s.	3	0.01 s.	7.29
Minus ($s = 1$)	23.2 s.	3	0.01 s.	16.71 s.
Minus ($s = 2$)	23.4 s.	3	0.01 s.	35.24 s.
Minus ($s = 3$)		*** Not possible ***		
Embedding ($r = 1$)	788 s.	3	0.01 s.	6.14 s.
Embedding ($r = 2$)	2811 s.	3	0.01 s.	5.25 s.
Embedding ($r = 3$)	401 s.	3	0.01 s.	4.44 s.

Kipnis-Shamir Attack vs. New Attack on HFE ($N = 1$)

Table: $q = 31, N = 1, D = 31^2 + 31 = 992$

d	6	7	8	9	10
KS attack (in s.)	0.54	14.1	16.1	20.3	73.8
new attack (in s.)	0.04	0.18	0.43	0.91	1.93
ratio	13.5	78.2	38.8	22.3	38.2

	11	12	13	14	15
	656	615	3524	2356	2966
	4.09	8.04	15.5	35.5	65.0
	160.3	76.5	228	66.4	45.6

Table: Proposed parameters of Multi-HFE. Broken on a 2.93 GHz Intel Xeon CPU.

q	N	d	D	security	d_{reg}(th.)	time (Magma)	mem (Magma)	d_{reg}
31	2	15	2	150 bits	4	2 m. 27 s.	434 MB	3
31	3	10	2	150 bits	4	1 h. 38 m.	1500 MB	3
31	3	15	2	192 bits	4	2 d. 1 h.	12 GB	3
31	3	18	2	256 bits	4	9 d. 16 h.	33 GB	3

q	N	d	D	security	d_{reg} (th.)	time (FGb)	mem (FGb)	d_{reg}
31	2	15	2	150 bits	4	21.1 s.	276.4 MB	3
31	3	10	2	150 bits	4	24 m. 56 s.	1589 MB	3
31	3	15	2	192 bits	4			
31	3	18	2	256 bits	4			

Outline

Introduction
- Presentation of HFE/Multi-HFE
- Known attacks
- The MinRank Problem

Attack on Multi-HFE
- Improvement and Extension of Kipnis-Shamir's attack
- Complexity Analysis
- Attacks on Multi-HFE Variants
- Experimental results

Conclusion
- Summary

Table: Status of HFE variants

construction	status	remarks
HFE ($N = 1$)	broken	Improved KS attack
multi-HFE ($N > 1$)	broken	Generalized attack
(multi-)HFE$^-$	not broken	broken if $s < (N-1)$
(multi-)HFE w/ emb.	broken	trick to recover $\mathbf{S}$
(multi-)HFEv	not broken	

Table: Status of HFE variants

construction	status	remarks
HFE ($N = 1$)	broken	Improved KS attack
multi-HFE ($N > 1$)	broken	Generalized attack
(multi-)HFE$^-$	not broken	broken if $s < (N-1)$
(multi-)HFE w/ emb.	broken	trick to recover $\mathbf{S}$
(multi-)HFEv	not broken	

Characteristic 2

- The attack does not work as described
- Issue when recovering S and T
- Adaptation of the attack in extended version.